SCHNEIDER DOWNS

Big Thinking. Personal Focus.

Demystifying HITRUST: A Practical Path to Clarity and Certification

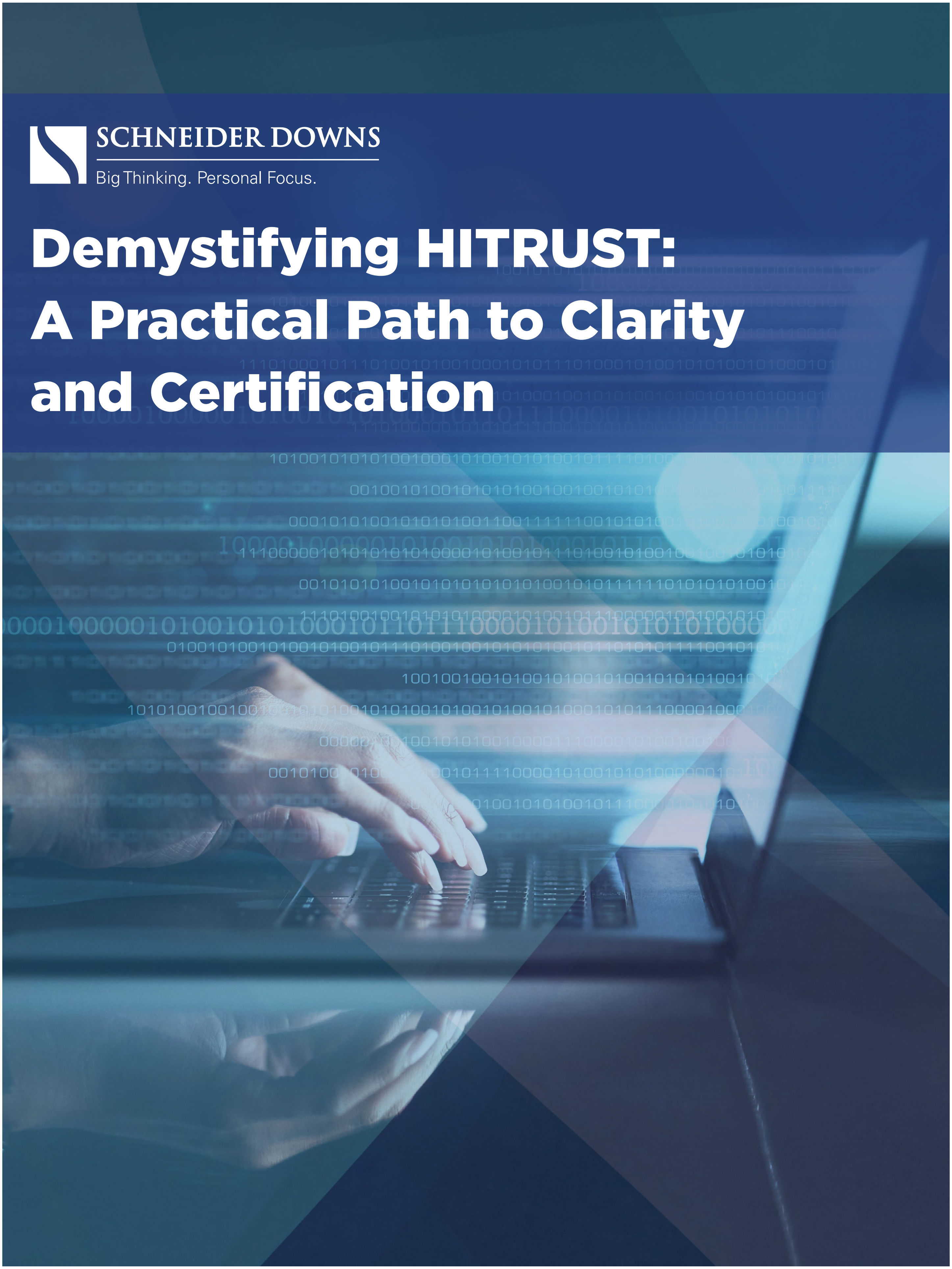

TABLE OF contents

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should not be relied upon when coordinated with individual professional advice.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Demystifying HITRUST: A Practical Path to Clarity and Certification

Understanding HITRUST

It's a bird! It's a plane! It's... HITRUST! But what exactly is HITRUST? Well, that is a complicated question.

HITRUST is a risk management framework, but it's also an organization. The HITRUST Alliance is a private entity that created the Common Security Framework (CSF), a certifiable framework that integrates and harmonizes various standards and regulations. The Alliance also developed supporting certifications (e1, i1, r2, etc.) and the MyCSF® assessment platform, a tool designed to streamline evaluations and reporting.

The HITRUST Alliance governs and supports the full ecosystem of its assurance programs. In short, it holds both the gavel and the sword when it comes to HITRUST programming.

At its core, HITRUST is an information protection standards organization and certifying body. Their mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries throughout the third-party supply chain.

While HITRUST CSF is industry-agnostic, it has become the gold standard for healthcare organizations seeking to demonstrate a serious commitment to security, privacy, and compliance. Still, with existing frameworks like HIPAA, SOC 2, NIST, PCI, and ISO already in use, many organizations understandably ask:

Is HITRUST really necessary?

What is HITRUST Certification?

HITRUST certification serves both as a recognized outcome and a powerful tool for demonstrating trust in an organization's security and privacy practices. It provides third-party assurance to customers and stakeholders that appropriate safeguards are in place.

To achieve this certification, HITRUST offers three core types of assessments, each tailored to an organization's size, risk profile, and assurance needs. All three assessment types are built on the HITRUST CSF, which integrates and harmonizes requirements from over 100 authoritative sources. These include HIPAA, NIST, COBIT, ISO 27001, SOC 2, and GDPR, combined into a single, scalable control framework. This allows organizations to address multiple compliance obligations through one comprehensive assessment. Here is a brief overview of the three progressive assessment and certification types:

Essentials, 1-Year (e1) assessment and certification for foundational cybersecurity

- Provides entry-level assurance focused on the most critical cybersecurity controls and demonstrates that essential cybersecurity hygiene is in place
- 44 controls testing "implementation" scoring only

Implemented, 1-Year (i1) assessment and certification for leading security practices (2 years with rapid recertification in year 2)

- Provides a moderate level of assurance that addresses cybersecurity leading practices and a broader range of active cyber threats than the e1 assessment
- 182 controls testing "implementation" scoring only

Risk-based, 2-Year (r2) assessment and certification for expanded practices (with an interim assessment in year 2)

- Provides a high level of assurance that focuses on a comprehensive risk-based specification of controls with an expanded approach to risk management and compliance evaluation
- ~375 controls, on average, testing "policy, procedure, and implementation" scoring

There are also new AI Security and Risk Management assessments and certifications, as well as the ability to add-on frameworks to the r2 certification and tailor it to your organization's needs.

How Does the HITRUST Process Work?

Understanding your customers' assurance needs is essential when selecting the appropriate HITRUST certification type. Regardless of which option you choose, the certification process is rigorous, standardized, and closely governed.

Every certification is reviewed and approved by the HITRUST Alliance. This level of oversight is critical. Without it, the certification would lose its credibility. This governance is often lacking in other standards-based frameworks. The structure and thoroughness of the HITRUST process are intentional, ensuring that the trust conveyed through certification is both consistent and meaningful.

The outcome of the certification is a validated assessment report and a certification badge, which can be used on your website, in documentation, or even in marketing materials. These are issued by the HITRUST Alliance through the MyCSF platform, in partnership with your certified External Assessor.

How HITRUST Compares to Other Frameworks

Framework	Purpose	Certifiable?	Mapped by HITRUST?
HIPAA	Privacy/security rule for healthcare	No	Yes
NIST 800-53	Federal security control catalog	No	Yes
SOC 2	Controls over service orgs (Trust Services Criteria)	Attestation, not certification	Yes
ISO 27001	InfoSec management system standard	Yes	Yes
CIS 18	Prioritized cybersecurity best practices	No	Yes
PCI-DSS	Payment card data security standard	Yes	Yes
COBIT	Governance and management of enterprise IT	No	Yes
GDPR	EU data protection regulation	No	Yes

Bottom line: HITRUST doesn't replace these, it consolidates and aligns them. Now that we understand what HITRUST is, let's debunk three common myths about what it isn't.

Debunking Common HITRUST Myths

We've covered what HITRUST is, how it works, and how it compares to other frameworks. Still, some common misconceptions remain. Here are three myths and the facts that set the record straight.

Myth 1: HITRUST is Just HIPAA with Extra Steps

That's like saying private health insurance is just Medicare with extra steps. HIPAA is a law. HITRUST is both an organization and a certifiable framework that maps to HIPAA but goes far beyond it. The HITRUST CSF integrates requirements from numerous standards and regulations, offering a comprehensive approach to risk management.

Myth 2: Only Large Enterprise Companies Need HITRUST

News flash: large enterprises do not assess third-party risk based solely on your revenue or employee count. If you process electronic protected health information (ePHI) on their behalf, they care about your security posture regardless of your size. Fortunately, HITRUST offers assessment types like e1 and i1 that are designed specifically for small and mid-sized businesses.

Myth 3: HITRUST is Just a Compliance Checkbox

This phrase alone will be sure to set off some Governance, Risk management, and Compliance (GRC) professionals. Organizations that treat compliance as a box to check often struggle or fall short. HITRUST is about maturity, not minimalism. It focuses on building a resilient security and privacy program that can evolve with threats and regulations.

So, Do You Really Need HITRUST?

Let's be honest. HITRUST is not a one-size-fits-all solution. But if you operate in healthcare or a related field, especially if you handle (e)PHI, it might be exactly the trust signal your organization needs. You should consider HITRUST if:

- **Your clients or prospects are asking for it.**
  Many large healthcare organizations and insurers require or strongly prefer HITRUST certification.
- **You are juggling multiple audits.**
  HITRUST can streamline compliance by aligning with frameworks such as HIPAA, SOC 2, PCI, NIST, and ISO.
- **You are scaling your business.**
  Expanding into new markets or launching new services? HITRUST shows that you take security and privacy seriously.
- **You want to stand out.**
  In a crowded and regulated market, HITRUST can serve as a strong differentiator.

You might wait if:

- You are a small operation without immediate compliance needs.
- Your clients are not requesting HITRUST, and your current framework is sufficient.

If you are considering HITRUST, start by evaluating your organization's needs and the expectations of your clients. Engage stakeholders across departments to understand the scope and impact. HITRUST certification is a long-term investment. It requires coordination, a clear understanding of your risk environment, and ongoing commitment across internal and external teams. Approach it as a journey and trust the process.

Build a HITRUST-Ready Program Without the Burnout

Many teams underestimate what's involved in HITRUST readiness until they're buried in policy updates, access logs, and endless evidence reviews. But with the right strategy, you can stay focused and maintain momentum all the way to certification. Here are five key tips to ensure you design a long-term foundation for your program.

Tip 1: Map Existing Controls First

A full control overhaul is not always necessary when working toward HITRUST. Your team is likely already doing much of the right work. It just may not be aligned with HITRUST terminology.

- If you have SOC 2, ISO 27001, or PCI in place, begin with HITRUST's authoritative source mappings and validate them against your existing controls.
- Focus on strong policies, consistent execution, and documentation that is clear and audit-ready.
- Use the requirement statements, evaluative elements, and illustrative procedures as your guide. These are the criteria used in certification and the best place to focus your efforts.

Tip 2: Use Automation to Your Advantage

Automation and repeatability are your best friends when building a sustainable compliance program. Let them help you.

- Leverage GRC platforms, ticketing systems, and cloud-native tools to minimize manual work.
- Automate tasks like alerts, evidence collection, and log reviews wherever possible. Make sure your external assessor is aligned with your automation strategy. A strong firm will recognize and account for efficiencies in their scoping and pricing.
- Create a centralized documentation repository early. It can save you hours, or even days, during validation and assessment.

Tip 3: Define Responsibilities and Control Owners

We've all been there – a last-minute scramble to gather evidence before deadlines. Well defined and clearly communicated responsibilities help spread the load and prevent any scrambles to gather evidence or meet deadlines.

- Designate a project manager or compliance lead
- Align specific controls to domain experts (IT, HR, Legal, DevOps)
- Avoid the burnout that comes from one person trying to "own" it all

Tip 4: Take a Phased Approach

New frameworks can feel overwhelming, but they become manageable when broken into smaller, focused stages. A structured, step-by-step approach helps reduce risk and keeps the project moving forward.

- Start with foundational domains (Access Control, Change Management, Risk Management, etc.)
- Use a phased roadmap (90-day increments) with clear progress tracking
- Communicate wins early and often to keep stakeholders engaged

Tip 5: Know When to Bring in Expert Support

Every organization has different strengths. When you hit a challenge outside your team's expertise, bring in experienced partners. The right advisor can help you avoid missteps, reduce rework, and accelerate your path to certification.

- Internal teams often don't have bandwidth or HITRUST expertise, and that's OK!
- Co-sourcing with a trusted advisor allows your team to stay focused on operations
- Advisors bring structure, tools, templates, and proven experience

Stay Focused on the Big Picture

HITRUST certification is a strategic effort that requires time, coordination, and sustained focus. With a strong plan, clear communication, and the right resources, your team can navigate the process confidently while maintaining momentum and executive support throughout.

How Can Schneider Downs Help?

As an Authorized HITRUST External Assessor Firm, Schneider Downs has a strong track record with HITRUST protocols, providing trusted guidance and support throughout the certification process. For more information, contact our HITRUST team at: **contactsd@schneiderdowns.com**.

About IT Risk Advisory

Schneider Downs' team of experienced risk advisory professionals focus on collaborating with your organization to identify and effectively mitigate risks. Our goal is to understand not only the risks related to potential loss to the organization, but to drive solutions that add value to your organization and advise on opportunities to ensure minimal disruption to your business.